

4F-1 侵入検知に対する対策の自動解除

大越丈弘

三菱電機株式会社 情報技術総合研究所

木下洋輔

三菱電機株式会社 通信機製作所

1. はじめに

情報システムへの不正侵入といった脅威に対抗して、侵入検知ツールが開発されている。どのツールも基本的には、侵入を検知すると通知するだけである。FW、ルータと連携してパケットを遮断するものもあるが、再び通信可能とするためには、コマンドによる指示又は再起動といった管理者の操作が必要となる。侵入防止のために自動的に通信が遮断されることは、対策として有効であるが、通信が遮断されたままでは業務に必要な通信が再開されず業務に支障をきたす。攻撃に対処しつつ円滑にサービスを提供するためには、不正な侵入が行われていなければただちにサービスに必要な通信が再開されなくてはならない。そこで我々は、侵入検知を行うだけでなく、実施した対策の解除が必要な場合には、対策の解除を管理者の手を煩わすことなく行うことで、サービスの可用性を向上させることを目標に検討を行った。

本稿は、対策の自動解除の機能について報告する。

2. 設計方針

2.1 侵入検知システム^[1]

一般には、検査対象のホスト上でホスト宛のパケットを分析するホスト型と、ネットワーク上のパケットを分析するネットワーク型に別れる。

ホスト型では、自分宛のパケットだけを分析するため、特定のプロトコル・アプリケーションでパケット分析処理を追加することにより、木目の細かい分析が可能となるが、すべてのホストへの侵入検知機能のセッティング、処理追加による他システムの影響（既存システムの変更）等、コスト及び作業が発生する場合がある。

一方、ネットワーク型は、ネットワーク上を流れるパケットを分析するため、既存システムの変更は

ないが、複数パケットによる攻撃や、分析処理速度により分析パケットの取りこぼしといった課題があり得る。

どちらの侵入検知システムも万能ではないため、ユーザは、組織の目的、リスク分析といったセキュリティポリシーによって組み合わせて使う。

2.2 攻撃と対策

攻撃には、アプリケーションの不具合を利用したもの、大量のパケットを集中的に流すことでサービスを不能とするサービス不能攻撃（Denial of Service、以降 DoS と略記。）等があり、その実施の方法はさまざまである。

また、攻撃に対する対策の一つは、プログラムの脆弱点にパッチをあてるなどのバージョンアップや、利用していないサービスの停止がある。これらの対策には、常日頃から攻撃とその対処についての情報収集を怠ってはいけな。また、他の対策として、DoS のような攻撃には、ルータやファイアーウォールなどで特定のパケットの遮断をすることも有効である。すなわち、攻撃によって日頃のメンテナンス（運用、手作業発生）で対応すべきもの、ネットワーク遮断等により一時的に対応すべきものがある。

2.3 設計方針

図1に、想定したネットワーク構成を示す。

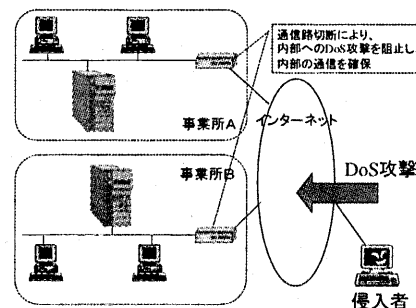


図1 ネットワーク構成

本検討における侵入検知機能は、既知の攻撃も検知することとする。そして、対策の実施及び解除を

行う攻撃は、ソフトウェアのバージョンアップといった管理者のメンテナンスだけでは対処できない DoS 攻撃とした。

また、実施する対策は、DoS 攻撃に対して有効で DoS 攻撃中だけ実施しなくてはならないことからネットワークの遮断とし、ソフトウェアのバージョンアップ等管理者による作業が不可欠なものについては対象外とした。なお、ネットワーク遮断により外部との通信は不可能となるが、攻撃によりネットワーク内部のサービスが停止しないことを優先させることとした。

そして、既存のネットワークシステム構成の変更を不要とするために、侵入検知システムは、ネットワーク型とした。

3. 実現方式

本設計では、パケットを遮断することから侵入検知部はルータに実装することとした。侵入検知部は、ネットワークから受信したパケットを分析し、対策の実施及び解除をルーティング部に通知する。図2に全体構成図を示す。

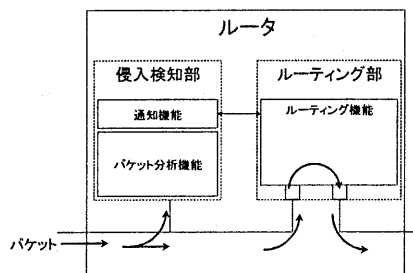


図2 全体構成図

3.1 DoS の検知方法

既知の DoS 攻撃のうち、同一送信元から大量のパケットを送信する攻撃を統計的な手法により検知する。すなわち、一定時間内に一定量受信した場合、DoS 攻撃と判断する。

3.2 対策

DoS 攻撃を検知した場合、侵入検知部は、ルーティング部に通知し、ルーティング機能において、パケットを廃棄（物理ポートをクローズ）することによって通信を遮断する。図3に、対策実施時のパ

ケット破棄に関する図を示す。

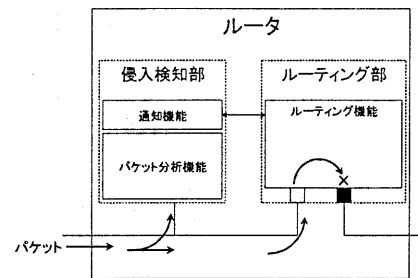


図3 対策実施時のパケットの破棄

3.3 対策実施中の攻撃パケットの監視

対策実施中、図3において、パケット分析機能は、同一送信元から同一パケット（攻撃パケット）が一定時間内に一定量あるか否かを監視する。

3.4 対策の解除

上述の監視において、攻撃パケットが一定量に達してなかった場合、ルーティング部に通知する。ルーティング部は、ルーティング機能によって、図2のように再びパケットを通過させることで対策を解除（物理ポートをオープン）する。

4. 今後の評価及び検討課題

本システムを用いて、実際に実施された対策解除の頻度及び管理者による作業に関する効果を検証しなくてはならない。

また、現状のパケット廃棄による対策では、全パケットを遮断してしまうため正常なパケットも通信不可となる。そのため、特定パケットだけを廃棄して正常なパケットを通過させることにより、機能を充実させてサービスの可用性をより向上させなくてはならない。

5. 終わりに

本稿では、サービスの可用性を向上させるために、管理者の手を煩わせることなく、実施した対策を解除するための一手法を説明した。

現在、機能の実現を目指して開発を進めている。

参考文献

[1]ISO WD 15947, IT intrusion detection framework